arXiv:1004.2193v2 [math.NT] 25 Sep 2010

ON THE SIMPLEST SEXTIC FIELDS AND RELATED THUE EQUATIONS

AKINARI HOSHI

Abstract. We consider the parametric family of sextic Thue equations

$$x^6-2mx^5y-5(m+3)x^4y^2-20x^3y^3+5mx^2y^4+2(m+3)xy^5+y^6=\lambda$$

where $m\in\mathbb{Z}$ is an integer and λ is a divisor of $27(m^2+3m+9)$. We show that the only solutions to the equations are the trivial ones with $xy(x+y)(x-y)(x+2y)(2x+y)=0$.

1. Introduction

We consider the following "simple" family of sextic Thue equations

$$\begin{aligned}F_m(X,Y):=\ &X^6-2mX^5Y-5(m+3)X^4Y^2\\ &-20X^3Y^3+5mX^2Y^4+2(m+3)XY^5+Y^6=\lambda\end{aligned}\tag{1}$$

for $m,\ \lambda\in\mathbb{Z}$ with $\lambda\neq 0$. We may assume that $m\geq -1$ because if $F_m(x,y)=\lambda$ then $F_{-m-3}(y,x)=\lambda$. If $(x,y)\in\mathbb{Z}^2$ is a solution to (1) then

$$(x+y,-x),\ (y,-x-y),\ (-x,-y),\ (-x-y,x),\ (-y,x+y)$$

are also solutions to (1) because $F_m(X,Y)$ is invariant under the action of the cyclic group $C_6=\langle\sigma\rangle$ of order 6 where $\sigma: X\mapsto X+Y,\, Y\mapsto -X$. For sextic integer $\lambda=e^6$ or $\lambda=-27e^6$, the equation $F_m(X,Y)=\lambda$ has the following six solutions respectively

$$\begin{aligned}F_m(0,\pm e)=F_m(\pm e,0)=F_m(\pm e,\mp e)=e^6,\\ F_m(\pm e,\pm e)=F_m(\pm 2e,\mp e)=F_m(\pm e,\mp 2e)=-27e^6.\end{aligned}$$

We call such solutions $(x,y)\in\mathbb{Z}^2$ to $F_m(x,y)=\lambda$ with $xy(x+y)(x-y)(x+2y)(2x+y)=0$ the *trivial* solutions. We remark that $F_m(2x+y,-x+y)=-27F_m(x,y)$.

For $m\geq 89$, Lettl-Pethö-Voutier [LPV99] showed that the only primitive solutions $(x,y)\in\mathbb{Z}^2$, i.e. $\gcd(x,y)=1$, to the Thue inequality $|F_m(x,y)|\leq 120m+323$ are

$$\begin{aligned}F_m(0,\pm 1)=F_m(\pm 1,0)\quad&=F_m(\pm 1,\mp 1)=1,\\ F_m(\pm 1,\pm 1)=F_m(\pm 2,\mp 1)&=F_m(\pm 1,\mp 2)=-27\end{aligned}\tag{2}$$

(i.e. trivial solutions) and

$$\begin{aligned}F_m(\pm 1,\pm 2)=F_m(\pm 3,\mp 1)=F_m(\pm 2,\mp 3)=120m+37,\\ F_m(\pm 2,\pm 1)=F_m(\pm 3,\mp 2)=F_m(\pm 1,\mp 3)=-120m-323.\end{aligned}$$

2000 *Mathematics Subject Classification.* Primary 11D41, 11D59, 11R20, 11Y40, 12F10.

Key words and phrases. Sextic Thue equations, simplest sextic fields, field isomorphism problem, multi-resolvent polynomial.

This work was partially supported by Rikkyo University Special Fund for Research and by the Grant-in-Aid for Young Scientists (B) No. 22740028, The Ministry of Education, Culture, Sports, Science and Technology, Japan.

In [LPV98], moreover, they obtained that for any $m \in \mathbb{Z}$ the equation $F_m(X,Y) = \lambda$ for $\lambda \in \{\pm 1, \pm 27\}$ has only twelve trivial solutions as in (2). A special case of $F_m(X,Y) = 1$ is also studied by Togbé [Tog02]. Wakabayashi [Wak07b] investigated Thue inequalities $|F_{l,m}(x,y)| \le k$ with two parameters l, m and $F_{1,m} = F_m$. The following is the main result of this paper (cf. cubic case [H1] and quartic case [H2]):

Theorem 1.1. *For $m \in \mathbb{Z}$ and a divisor λ of $27(m^2+3m+9)$, the only solutions to the equation $F_m(x,y) = \lambda$ are the trivial ones with $xy(x+y)(x-y)(x+2y)(2x+y) = 0$.*

We take the simplest sextic polynomial

$$f_m^{C_6}(X) := X^6 - 2mX^5 - 5(m+3)X^4 - 20X^3 + 5mX^2 + 2(m+3)X + 1 \in \mathbb{Q}[X]$$

with discriminant $6^6(m^2+3m+9)^5$. Note that $f_m^{C_6}(X) = F_m(X,1)$.

For $m \in \mathbb{Z} \setminus \{-8,-3,0,5\}$, the polynomial $f_m^{C_6}(X)$ is irreducible over $\mathbb{Q}$ with cyclic Galois group $\mathrm{Gal}_{\mathbb{Q}} f_m^{C_6}(X) \cong C_6$ of order 6 (see [Gra86, Proposition 3.3]). The splitting fields

$$L_m^{(6)} := \mathrm{Spl}_{\mathbb{Q}} f_m^{C_6}(X), \quad (m \in \mathbb{Z} \setminus \{-8,-3,0,5\})$$

of $f_m^{C_6}(X)$ over $\mathbb{Q}$ are totally real cyclic sextic fields and called the simplest sextic fields (cf. e.g. [Gra86], [Gra87], [LPV98], [LPV99], [Gaa02, Section 8.3], [Tog02], [HH05], [Lou07]).

We get Theorem 1.1 as a consequence of the following two theorems:

Theorem (Theorem 4.7)**.** *For $m, n \in \mathbb{Z}$, $L_m^{(6)} = L_n^{(6)}$ if and only if $m = n$ or $m = -n-3$.*

Theorem (Theorem 5.1)**.** *There exists an integer $n \in \mathbb{Z} \setminus \{m, -m-3\}$ such that $L_n^{(6)} = L_m^{(6)}$ if and only if there exists non-trivial solution $(x,y) \in \mathbb{Z}^2$, i.e. $xy(x+y)(x-y)(x+2y)(2x+y) \neq 0$, to $F_m(x,y) = \lambda$ where λ is a divisor of $27(m^2+3m+9)$.*

In Section 2, we review some facts on the simplest sextic and cubic fields. In Section 3, we recall known results of the resolvent polynomials which are fundamental tools in the computational aspects of Galois theory. We intend to explain how to obtain an answer to the field intersection problem of cyclic sextic polynomials $f_s(X)$ over a field K of char $K \neq 2, 3$, i.e. for $a, b \in K$ how to determine the intersection of $\mathrm{Spl}_K f_a(X)$ and $\mathrm{Spl}_K f_b(X)$. In Section 4, we give an explicit answer to the field isomorphism problem of $f_s^{C_6}(X)$ as the special case of the field intersection problem. In particular, for $K = \mathbb{Q}$, we get Theorem 4.7 by using Okazaki's theorem (Theorem 2.1). In Section 5, we will show a correspondence between isomorphism classes of the simplest sextic fields $L_m^{(6)}$ and non-trivial solutions to the sextic Thue equations $F_m(x,y) = \lambda$ where λ is a divisor of $27(m^2+3m+9)$ (see Theorem 5.1).

2. The simplest sextic and cubic fields

We recall known facts of the simplest sextic and cubic fields (see [Gra86, Section 3], [Gra87], [LPV98]).

Let K be a field of char $K \neq 2, 3$ and $K(s)$ the rational function field over K with variable s. We take the simplest sextic polynomial

$$f_s^{C_6}(X) := X^6 - 2sX^5 - 5(s+3)X^4 - 20X^3 + 5sX^2 + 2(s+3)X + 1$$

with discriminant $6^6(s^2+3s+9)^5$. The Galois group of $f_s^{C_6}(X)$ over $K(s)$ is isomorphic to the cyclic group C_6 of order 6. Gras [Gra86] considered the polynomial

$$g_t(X) = X^6 - \frac{1}{2}(t-6)X^5 - \frac{5}{4}(t+6)X^4 - 20X^3 + \frac{5}{4}(t-6)X^2 + \frac{1}{2}(t+6)X + 1.$$

The two polynomials above are related by $g_{4s+6}(X) = f_s^{C_6}(X)$.

Let $K(z)$ be the rational function field over K with variable z and σ a K-automorphism of $K(z)$ of order 6 which is defined by

$$\sigma : z \mapsto \frac{z-1}{z+2} \mapsto -\frac{1}{z+1} \mapsto -\frac{z+2}{2z+1} \mapsto -\frac{z+1}{z} \mapsto -\frac{2z+1}{z-1} \mapsto z. \tag{3}$$

Then we get the Galois extension $K(z)/K(z)^{\langle\sigma\rangle}$ with cyclic Galois group C_6 of order 6 and

$$f_s^{C_6}(X) = \prod_{x \in \mathrm{Orb}_{\langle\sigma\rangle}(z)} \Big(X - x\Big)$$

where

$$s = \frac{z^6 - 15z^4 - 20z^3 + 6z + 1}{z(2z^4 + 5z^3 - 5z - 2)} = \frac{(z^3 + 3z^2 - 1)(z^3 - 3z^2 - 6z + 1)}{z(z+1)(z-1)(z+2)(2z+1)}$$

as the generating polynomial of the sextic cyclic field $K(z)$ over $K(z)^{\langle\sigma\rangle} = K(s)$.

The quadratic field $K(z)^{\langle\sigma^2\rangle}$ over $K(s)$ is given by $K(s)(z_2)$ where

$$z_2 = z + \sigma^2(z) + \sigma^4(z) = \frac{z^3 - 3z - 1}{z(z+1)}.$$

It also follows from

$$z_2 - s = \frac{(z^2 + z + 1)^3}{z(z+1)(z-1)(z+2)(2z+1)} = \sqrt{s^2 + 3s + 9} \tag{4}$$

that $K(z)^{\langle\sigma^2\rangle} = K(s)(\sqrt{s^2 + 3s + 9})$.

The cyclic cubic field $K(z)^{\langle\sigma^3\rangle}$ over $K(s)$ is given by $K(s)(z_3)$ where

$$z_3 = \frac{1}{z\,\sigma^3(z)} = -\frac{z(z+2)}{(z+1)(z-1)}.$$

The action of σ on $K(s)(z_3)$ is given by

$$\sigma : s \mapsto s,\ z_3 \mapsto -\frac{1}{z_3 + 1} \mapsto -\frac{z_3 + 1}{z_3} \mapsto z_3.$$

Hence the minimal polynomial of z_3 over $K(s)$ is given by

$$f_s^{C_3}(X) := \prod_{x \in \mathrm{Orb}_{\langle\sigma\rangle}(z_3)} \Big(X - x\Big) = X^3 - sX^2 - (s+3)X - 1,$$

that is the simplest cubic polynomial of Shanks [Sha74]. Two polynomials $f_s^{C_6}(X)$ and $f_s^{C_3}(X)$ satisfy the relation

$$f_s^{C_6}(X) = (f_s^{C_3}(X))^2 - (s^2 + 3s + 9)X^2(X+1)^2. \tag{5}$$

For $K = \mathbb{Q}$, we consider the specialization map $s \mapsto m \in \mathbb{Z}$. By [Gra86, Proposition 3.3], the sextic polynomial $f_m^{C_6}(X)$ is irreducible over $\mathbb{Q}$ for $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$, and the splitting fields $L_m^{(6)} = \mathrm{Spl}_{\mathbb{Q}} f_m^{C_6}(X)$ are totally real cyclic number fields of degree 6 which are called the simplest sextic fields. We see $L_m^{(6)} = L_{-m-3}^{(6)}$ because if z is a root of $f_m^{C_6}(X)$ then $1/z$ becomes a root of $f_{-m-3}^{C_6}(X)$.

For $m \in \{-8, -3, 0, 5\}$, an integer $m^2 + 3m + 9$ is square and then from (4) and (5) the sextic polynomial $f_m^{C_6}(X)$ splits over $\mathbb{Q}$. Indeed we see

$$f_{-8}^{C_6}(X) = f_{-1}^{C_3}(X) f_{-15}^{C_3}(X), \qquad f_{-3}^{C_6}(X) = f_0^{C_3}(X) f_{-6}^{C_3}(X),$$
$$f_0^{C_6}(X) = f_3^{C_3}(X) f_{-3}^{C_3}(X), \qquad f_5^{C_6}(X) = f_{12}^{C_3}(X) f_{-2}^{C_3}(X).$$

The cubic subfields $L_m^{(3)} := \mathrm{Spl}_{\mathbb{Q}} f_m^{C_3}(X)$ of $L_m^{(6)}$ are called the simplest cubic fields. Note that $f_m^{C_3}(X)$ is irreducible over $\mathbb{Q}$ and $L_m^{(3)} = L_{-m-3}^{(3)}$ for any $m \in \mathbb{Z}$.

Ennola [Enn91] verified that for integers $-1 \leq m < n \leq 10^4$, $L_m^{(3)} = L_n^{(3)}$ if and only if $(m,n) \in \{(-1,5),\ (-1,12),\ (-1,1259),\ (5,12),\ (5,1259),\ (12,1259)\} \cup \{(0,3),\ (0,54),\ (3,54)\} \cup \{(1,66)\} \cup \{(2,2389)\}$. Hoshi-Miyake [HM09a, Example 5.3] checked that Ennola's claim is also valid for $-1 \leq m < n \leq 10^5$.

In [Oka02], Okazaki investigated Thue equations $F(X,Y) = 1$ for irreducible cubic forms F with positive discriminant $D(F) > 0$ and established a very strong result on gaps between solutions (cf. also [Wak07a]). By using methods in [Oka02], we may obtain that if $L_m^{(3)} = L_n^{(3)}$ with $-1 \leq m < n$ then $m \leq 35731$ (cf. also [H1]). Moreover Okazaki showed the following theorem:

Theorem 2.1 (Okazaki [Oka]). *Let $L_m^{(3)} = \mathrm{Spl}_{\mathbb{Q}} f_m^{C_3}(X)$. For $m, n \in \mathbb{Z}$ with $-1 \leq m < n$, if $L_m^{(3)} = L_n^{(3)}$ then $m, n \in \{-1,\ 0,\ 1,\ 2,\ 3,\ 5,\ 12,\ 54,\ 66,\ 1259,\ 2389\}$. In particular,*

$$L_{-1}^{(3)} = L_5^{(3)} = L_{12}^{(3)} = L_{1259}^{(3)}, \quad L_0^{(3)} = L_3^{(3)} = L_{54}^{(3)}, \quad L_1^{(3)} = L_{66}^{(3)}, \quad L_2^{(3)} = L_{2389}^{(3)}.$$

The author also gave an another proof of Theorem 2.1 in [H1].

3. Field intersection problem of cyclic sextic

We recall some results of the resolvent polynomials which are fundamental tools in the computational aspects of Galois theory (cf. e.g. [Coh93], [Coh00], [Ade01]). Let $\overline{K}$ be a fixed algebraic closure of a field K. Let $f(X) := \prod_{i=1}^m (X - \alpha_i) \in K[X]$ be a separable polynomial of degree m with some fixed order of the roots $\alpha_1, \ldots, \alpha_m \in \overline{K}$. The Galois group of the polynomial $f(X)$ over K may be determined by resolvent polynomials with suitable invariants.

Let $R := K[x_1, \ldots, x_m]$ be the polynomial ring over K with m variables $x_1, \ldots, x_m$. For $\Theta \in R$, we take the specialization map $\omega_f : R \to k(\alpha_1, \ldots, \alpha_m)$, $\Theta(x_1, \ldots, x_m) \mapsto \Theta(\alpha_1, \ldots, \alpha_m)$. The kernel of ω_f is the ideal $I_f := \{\Theta \in R \mid \Theta(\alpha_1, \ldots, \alpha_m) = 0\}$ in R.

Let S_m be the symmetric group of degree m. We extend the action of S_m on m letters $\{1, \ldots, m\}$ to that on R by $\pi(\Theta(x_1, \ldots, x_m)) := \Theta(x_{\pi(1)}, \ldots, x_{\pi(m)})$. The Galois group of $f(X)$ over K is defined by $\mathrm{Gal}(f/K) := \{\pi \in S_m \mid \pi(I_f) \subseteq I_f\}$, and $\mathrm{Gal}(f/K)$ is isomorphic to the Galois group of the splitting field $\mathrm{Spl}_K f(X)$ of $f(X)$ over K. If we take another ordering of roots $\alpha_{\pi(1)}, \ldots, \alpha_{\pi(m)}$ of $f(X)$ for some $\pi \in S_m$, the corresponding realization of $\mathrm{Gal}(f/K)$ is conjugate in S_m. Hence, for arbitrary ordering of the roots of $f(X)$, $\mathrm{Gal}(f/K)$ is determined up to conjugacy in S_m.

For $H \leq U \leq S_m$, an element $\Theta \in R$ is called a U-primitive H-invariant if $H = \mathrm{Stab}_U(\Theta)$ $:= \{\pi \in U \mid \pi(\Theta) = \Theta\}$. For a U-primitive H-invariant Θ, the polynomial

$$\mathcal{RP}_{\Theta,U}(X) = \prod_{\overline{\pi} \in U/H} (X - \pi(\Theta)) \in R^U[X]$$

where $\overline{\pi}$ runs through the left cosets of H in U, is called the *formal* U-relative H-invariant resolvent by Θ. The polynomial

$$\mathcal{RP}_{\Theta,U,f}(X) := \omega_f(\mathcal{RP}_{\Theta,U}(X))$$

is called the U-relative H-invariant resolvent of f by Θ. The following theorem is fundamental in the theory of resolvent polynomials (see e.g. [Ade01, p.95]).

Theorem 3.1. *Let $G = \mathrm{Gal}(f/K)$, $H \le U \le S_m$ be finite groups with $G \le U$ and Θ a U-primitive H-invariant. Suppose that $\mathcal{RP}_{\Theta,U,f}(X) = \prod_{i=1}^{l} h_i^{e_i}(X)$ gives the decomposition of $\mathcal{RP}_{\Theta,U,f}(X)$ into a product of powers of distinct irreducible polynomials $h_i(X)$, $(i = 1, \ldots, l)$, in $K[X]$. Then we have a bijection*

$$\begin{array}{rcl} G\backslash U/H & \longrightarrow & \{h_1^{e_1}(X), \ldots, h_l^{e_l}(X)\} \\ G\,\pi\,H & \longmapsto & h_\pi(X) = \displaystyle\prod_{\tau H \subseteq G\,\pi\,H} \big(X - \omega_f(\tau(\Theta))\big) \end{array}$$

where the product runs through the left cosets τH of H in U contained in $G\,\pi\,H$, that is, through $\tau = \pi_\sigma \pi$ where π_σ runs a system of representative of the left cosets of $G \cap \pi H \pi^{-1}$; each $h_\pi(X)$ is irreducible or a power of an irreducible polynomial with $\deg(h_\pi(X)) = |G\,\pi\,H|/|H|$ $= |G|/|G \cap \pi H \pi^{-1}|$.

Corollary 3.2. *If $G \le \pi H \pi^{-1}$ for some $\pi \in U$ then $\mathcal{RP}_{\Theta,U,f}(X)$ has a linear factor over K. Conversely, if $\mathcal{RP}_{\Theta,U,f}(X)$ has a non-repeated linear factor over K then there exists $\pi \in U$ such that $G \le \pi H \pi^{-1}$.*

Remark 3.3. When $\mathcal{RP}_{\Theta,U,f}(X)$ is not squarefree, there exists a suitable Tschirnhausen transformation $\hat{f}$ of f over K such that $\mathcal{RP}_{\Theta,U,\hat{f}}(X)$ is squarefree (cf. [Gir83], [Coh93, Alg. 6.3.4]).

Now we apply Theorem 3.1 to the cyclic sextic case. Let $f^1(X)$, $f^2(X) \in K[X]$ be separable sextic polynomials over K. We put

$$f(X) := f^1(X) f^2(X), \quad G_i := \mathrm{Gal}(f^i/K), \quad L_i := \mathrm{Spl}_K f^i(X), \quad (i = 1, 2).$$

We assume that $G_1, G_2 \le C_6$ and apply Theorem 3.1 to $m = 12$, $f(X) = f^1(X) f^2(X)$, $U = \langle \sigma \rangle \times \langle \tau \rangle$, $H = \langle \sigma\tau \rangle$ or $\langle \sigma\tau^5 \rangle$ where $\sigma, \tau \in S_{12}$ act on $R = K[x_1, \ldots, x_{12}]$ by

$$\sigma : x_1 \mapsto x_2 \mapsto \cdots \mapsto x_6 \mapsto x_1, \quad \tau : x_7 \mapsto x_8 \mapsto \cdots \mapsto x_{12} \mapsto x_7.$$

Let Θ_1 (resp. Θ_2) be a U-primitive $\langle \sigma\tau \rangle$-invariant (resp. $\langle \sigma\tau^5 \rangle$-invariant) where $U = \langle \sigma \rangle \times \langle \tau \rangle$. Then the U-relative $\langle \sigma\tau \rangle$-invariant (resp. $\langle \sigma\tau^5 \rangle$-invariant) resolvent polynomial of $f(X) = f^1(X) f^2(X)$ by Θ_1 (resp. Θ_2) is given by

$$\mathcal{R}_f^i(X) := \mathcal{RP}_{\Theta_i,U,f}(X), \quad (i = 1, 2).$$

This is also called (absolute) *multi-resolvent polynomial* (cf. [RV99], [Ren04]).

For a squarefree polynomial $\mathcal{R}(X) \in K[X]$ of degree l, we define the *decomposition type* $\mathrm{DT}(\mathcal{R})$ of $\mathcal{R}(X)$ by the partition of l induced by the degrees of the irreducible factors of $\mathcal{R}(X)$ over K. By Theorem 3.1, we get the intersection field $L_1 \cap L_2$ via the decomposition types $\mathrm{DT}(\mathcal{R}_f^1)$ and $\mathrm{DT}(\mathcal{R}_f^2)$.

Theorem 3.4. *For $f(X) = f^1(X) f^2(X) \in K[X]$ with G_1, $G_2 \le C_6$, we assume that $\#G_1 \ge \#G_2$ and both $\mathcal{R}_f^1(X)$ and $\mathcal{R}_f^2(X)$ are squarefree. Then the Galois group $G = \mathrm{Gal}(f/K)$ and the intersection field $L_1 \cap L_2$ are given by the decomposition types* $\mathrm{DT}(\mathcal{R}_f^1)$ *and* $\mathrm{DT}(\mathcal{R}_f^2)$ *as on Table* 1.

Table 1

G_1	G_2	G		$\mathrm{DT}(\mathcal{R}_f^1)$	$\mathrm{DT}(\mathcal{R}_f^2)$
C_6	C_6	$C_6 \times C_6$	$L_1 \cap L_2 = K$	6	6
		$C_6 \times C_3$	$[L_1 \cap L_2 : K] = 2$	$3,3$	$3,3$
		$C_6 \times C_2$	$[L_1 \cap L_2 : K] = 3$	6	$2,2,2$
				$2,2,2$	6
		C_6	$L_1 = L_2$	$3,3$	$1,1,1,1,1,1$
				$1,1,1,1,1,1$	$3,3$
	C_3	$C_6 \times C_3$	$L_1 \cap L_2 = K$	6	6
		C_6	$L_1 \supset L_2$	6	$2,2,2$
				$2,2,2$	6
	C_2	$C_6 \times C_2$	$L_1 \cap L_2 = K$	6	6
		C_6	$L_1 \supset L_2$	$3,3$	$3,3$
	$\{1\}$	C_6	$L_1 \supset L_2 = K$	6	6
C_3	C_3	$C_3 \times C_3$	$L_1 \cap L_2 = K$	$3,3$	$3,3$
		C_3	$L_1 = L_2$	$3,3$	$1,1,1,1,1,1$
				$1,1,1,1,1,1$	$3,3$
	C_2	C_6	$L_1 \cap L_2 = K$	6	6
	$\{1\}$	C_3	$L_1 \supset L_2 = K$	$3,3$	$3,3$
C_2	C_2	$C_2 \times C_2$	$L_1 \cap L_2 = K$	$2,2,2$	$2,2,2$
		C_2	$L_1 = L_2$	$1,1,1,1,1,1$	$1,1,1,1,1,1$
	$\{1\}$	C_2	$L_1 \supset L_2$	$2,2,2$	$2,2,2$
$\{1\}$	$\{1\}$	$\{1\}$	$L_1 = L_2 = K$	$1,1,1,1,1,1$	$1,1,1,1,1,1$

We checked the decomposition types $\mathrm{DT}(\mathcal{R}_f^i)$, $(i = 1, 2)$, on Table 1 using the computer algebra system GAP [GAP] via the command `DoubleCosetRepsAndSizes`.

4. An explicit answer to the isomorphism problem

By using Theorem 3.4, we give an answer to the field intersection problem of

$$f_s^{C_6}(X) = X^6 - 2sX^5 - 5(s+3)X^4 - 20X^3 + 5sX^2 + 2(s+3)X + 1,$$

i.e. for $a, b \in K$ how to determine the intersection of $\mathrm{Spl}_K f_a(X)$ and $\mathrm{Spl}_K f_b(X)$, via multi-resolvent polynomials. An explicit answer to the field isomorphism problem of $f_s^{C_6}(X)$ will be given as the special case of the field intersection problem (see Theorem 4.3).

For $n \geq 3$, Rikuna [Rik02] constructed one-parameter families of cyclic polynomials $f_s^{R(n)}(X)$ of degree n over K with char $K \not| \, n$ and $K \ni \zeta_n + \zeta_n^{-1}$ where ζ_n is a primitive n-th root of unity. The simplest sextic polynomial $f_s^{C_6}(X)$ may be obtained as the sextic case $f_s^{R(6)}(X)$ (see also [Miy99], [HM99]).

Komatsu [Kom04] established descent Kummer theory via $f_s^{R(n)}(X)$, and gave a necessary and sufficient condition to $\mathrm{Spl}_K f_a^{R(n)}(X) \subset \mathrm{Spl}_K f_b^{R(n)}(X)$ for $a, b \in K$ (see also [Oga03], [Kid05]). It is interesting to compare the results of [Oga03], [Kom04], [Kid05] with results given in this section. We note that a method via multi-resolvent polynomials is valid also for non-abelian groups (see [HM07], [HM09b], [HM09c], [HM10c]).

Let K be a field of char $K \neq 2, 3$, $K(z)$ the rational function field over K with variable z and σ a K-automorphism of $K(z)$ of order 6 which is given by (3). We also take another rational function field $K(w)$ over K, a K-automorphism of $K(w)$ of order 6

$$\tau : w \ \mapsto\ \frac{w-1}{w+2} \ \mapsto\ -\frac{1}{w+1} \ \mapsto\ -\frac{w+2}{2w+1} \ \mapsto\ -\frac{w+1}{w} \ \mapsto\ -\frac{2w+1}{w-1} \ \mapsto\ w$$

and $f_t^{C_6}(X) = X^6 - 2tX^5 - 5(t+3)X^4 - 20X^3 + 5tX^2 + 2(t+3)X + 1$ where

$$t = \frac{w^6 - 15w^4 - 20w^3 + 6w + 1}{w(2w^4 + 5w^3 - 5w - 2)} = \frac{(w^3 + 3w^2 - 1)(w^3 - 3w^2 - 6w + 1)}{w(w+1)(w-1)(w+2)(2w+1)}$$

by the same manner of $K(z)$, σ and $f_s^{C_6}(X)$.

Then the field $K(z,w)$ is $(C_6 \times C_6)$-extension of $K(z,w)^U = K(s,t)$ where $U = \langle\sigma\rangle \times \langle\tau\rangle$. Now we should find suitable U-primitive $\langle\sigma\tau\rangle$-invariant Θ_1 (resp. $\langle\sigma\tau^5\rangle$-invariant Θ_2). By [AHK98, Theorem 1.4], there exists $\langle\sigma\tau\rangle$-invariant Θ_1 such that $K(z,w) = K(z,\Theta_1)$. Moreover we may obtain the following Θ_1 and Θ_2:

Lemma 4.1. *Let $U = \langle\sigma\rangle \times \langle\tau\rangle$,*

$$\Theta_1 = -\frac{zw + z + 1}{z - w} \quad \textit{and} \quad \Theta_2 = \frac{zw - 1}{z + w + 1}.$$

Then the following assertions hold:
(i) *the element Θ_1 is a U-primitive $\langle\sigma\tau\rangle$-invariant*;
(ii) *the element Θ_2 is a U-primitive $\langle\sigma\tau^5\rangle$-invariant*;
(iii) *the U-orbit of Θ_i is given by the same as $\langle\sigma\rangle$-orbit of z*;

$$\mathrm{Orb}_U(\Theta_i) = \left\{\Theta_i, \frac{\Theta_i - 1}{\Theta_i + 2}, -\frac{1}{\Theta_i + 1}, -\frac{\Theta_i + 2}{2\Theta_i + 1}, -\frac{\Theta_i + 1}{\Theta_i}, -\frac{2\Theta_i + 1}{\Theta_i - 1}\right\}, \quad (i = 1, 2).$$

Proof. We can check the assertions by direct computations. □

Put $f_{a,b}(X) := f_a^{C_6}(X) f_b^{C_6}(X)$. The multi-resolvent polynomials

$$\mathcal{R}^i_{f_{a,b}}(X) := \mathcal{RP}_{\Theta_i, \langle\sigma\rangle\times\langle\tau\rangle, f_{a,b}}(X), \quad (i = 1, 2)$$

with respect to Θ_1 and Θ_2 as in Lemma 4.1 are given by

$$\mathcal{R}^i_{f_{a,b}}(X) = f_{A_i}^{C_6}(X), \quad (i = 1, 2) \tag{6}$$

where

$$A_1 = -\frac{ab + 3a + 9}{a - b}, \quad A_2 = \frac{ab - 9}{a + b + 3}.$$

Note that

$$\mathrm{disc}(\mathcal{R}^1_{f_{a,b}}(X)) = \frac{6^6(a^2 + 3a + 9)^5(b^2 + 3b + 9)^5}{(a - b)^{10}},$$

$$\mathrm{disc}(\mathcal{R}^2_{f_{a,b}}(X)) = \frac{6^6(a^2 + 3a + 9)^5(b^2 + 3b + 9)^5}{(a + b + 3)^{10}}.$$

By Theorem 3.4, we get the intersection field $\mathrm{Spl}_K f_a^{C_6}(X) \cap \mathrm{Spl}_K f_b^{C_6}(X)$ via Table 1.

Theorem 4.2. *Let K be a field of char $K \neq 2, 3$ and $\mathcal{R}^i_{f_{a,b}}(X) = f_{A_i}^{C_6}(X)$, $(i = 1, 2)$, as in* (6). *For $a, b \in K$ with $(a - b)(a + b + 3) \neq 0$ and $(a^2 + 3a + 9)(b^2 + 3b + 9) \neq 0$, we assume that $\#\mathrm{Gal}_K f_a^{C_6}(X) \geq \#\mathrm{Gal}_K f_b^{C_6}(X)$. Then the intersection field $\mathrm{Spl}_K f_a^{C_6}(X) \cap \mathrm{Spl}_K f_b^{C_6}(X)$ is given by the decomposition types $\mathrm{DT}(\mathcal{R}^1_{f_{a,b}})$ and $\mathrm{DT}(\mathcal{R}^2_{f_{a,b}})$ as on Table* 1.

As the special case of Theorem 4.2, we obtain an explicit answer to the field isomorphism problem of $f_s^{C_6}(X)$.

Theorem 4.3. *Let K be a field of char $K \neq 2, 3$. For $a, b \in K$ with $(a-b)(a+b+3) \neq 0$ and $(a^2+3a+9)(b^2+3b+9) \neq 0$, the following three conditions are equivalent:*
(i) *the splitting fields of $f_a^{C_6}(X)$ and of $f_b^{C_6}(X)$ over K coincide;*
(ii) *the polynomial $f_{A_i}^{C_6}(X)$ splits completely into 6 linear factors over K for $i = 1$ or $i = 2$ where*

$$A_1 = -\frac{ab+3a+9}{a-b} \quad \textit{and} \quad A_2 = \frac{ab-9}{a+b+3};$$

(iii) *there exists $z \in K$ such that*

$$B = a + \frac{(a^2+3a+9)z(z+1)(z-1)(z+2)(2z+1)}{f_a(z)}$$

where $B = b$ or $B = -b-3$.

Moreover if $\mathrm{Gal}_K f_a^{C_6}(X) \cong C_6$ or C_3 (resp. $\mathrm{Gal}_K f_a^{C_6}(X) \cong C_2$ or $\{1\}$) then (ii) *occurs for only one of A_1 and A_2 (resp. for both of A_1 and A_2) and* (iii) *occurs for only one of b and $-b-3$ (resp. for both of b and $-b-3$).*

Remark 4.4. The condition (iii) is just a restatement of (ii). Indeed, for $i = 1, 2$, rational roots $z \in K$ of $f_{A_i}^{C_6}(X)$ satisfy the condition (iii) for $B = b$ and $B = -b-3$ respectively. The equivalence of the conditions (i) and (iii) is valid also for $a = b$ and $b = -a-3$.

Theorem 4.3 is a generalization of the results of the simplest cubic (resp. quartic) case in [Mor94], [Cha96], [HM09a] (resp. [H2]). This is an analogue of Kummer theory; for a field K which contains a primitive 6th root ζ_6 of unity and $a, b \in K$, $\mathrm{Spl}_K(X^6 - a) = \mathrm{Spl}_K(X^6 - b)$ if and only if $X^6 - ab$ or $X^6 - ab^5$ splits completely over K. It is remarkable that Theorem 4.3 does not need the assumption that K contains ζ_6.

By Theorem 4.3, for a fixed $a \in K$ with $a^2+3a+9 \neq 0$, we have $\mathrm{Spl}_K f_b^{C_6}(X) = \mathrm{Spl}_K f_a^{C_6}(X)$ where b is given as in Theorem 4.3 (iii) for arbitrary $z \in K$ with $f_a(z) \neq 0$ and $b^2+3b+9 \neq 0$.

Corollary 4.5. *Let K be an infinite field of char $K \neq 2$. For a fixed $a \in K$ with $a^2+3a+9 \neq 0$, there exist infinitely many $b \in K$ such that $\mathrm{Spl}_K f_b^{C_6}(X) = \mathrm{Spl}_K f_a^{C_6}(X)$.*

However, by applying Siegel's theorem for curves of genus 0 (cf. [Lan78, Theorem 6.1], [Lan83, Chapter 8, Section 5]) to Theorem 4.3 (iii), we get

Corollary 4.6. *Let K be a number field and $\mathcal{O}_K$ the ring of integers in K. Assume that $a \in \mathcal{O}_K$ with $a^2+3a+9 \neq 0$. Then there exist only finitely many integers $b \in \mathcal{O}_K$ such that $\mathrm{Spl}_K f_b^{C_6}(X) = \mathrm{Spl}_K f_a^{C_6}(X)$. In particular, there exist only finitely many integers $b \in \mathcal{O}_K$ such that $f_{A_i}^{C_6}(X)$, $(i = 1, 2)$, has a linear factor over $\mathbb{Q}$.*

When $K = \mathbb{Q}$, by Okazaki's theorem (Theorem 2.1) and Theorem 4.3 we have

Theorem 4.7. *Let $L_m^{(6)} = \mathrm{Spl}_{\mathbb{Q}} f_m^{C_6}(X)$. For $m, n \in \mathbb{Z}$, $L_m^{(6)} = L_n^{(6)}$ if and only if $m = n$ or $m = -n-3$.*

Proof. We should check the assertion only for $-1 \leq m < n$ and $m, n \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ because $L_m^{(3)}$ is the cubic subfield of $L_m^{(6)}$ and hence $L_m^{(6)} = L_n^{(6)}$ implies $L_m^{(3)} = L_n^{(3)}$ (cf. Theorem 2.1). The irreducible factorization of the corresponding multi-resolvent polynomials $\mathcal{R}^i_{f_{m,n}}(X) = f_{A_i}^{C_6}(X)$ over $\mathbb{Q}$ are given as on Table 2.

Table 2

m	n	i	irreducible factorization of $f_{A_i}^{C_6}(X)$ over $\mathbb{Q}$
-1	5	1	$(X^2-4X-3)(X^2+3X+\frac{1}{2})(X^2+\frac{2X}{3}-\frac{2}{3})$
-1	12	2	$(X^2-2X-2)(X^2+4X+1)(X^2+X-\frac{1}{2})$
-1	1259	1	$(X^2-\frac{5}{2}X-\frac{9}{4})(X^2+\frac{18}{5}X+\frac{4}{5})(X^2+\frac{8}{9}X-\frac{5}{9})$
5	12	2	$(X^2-8X-5)(X^2+\frac{5}{2}X+\frac{1}{4})(X^2+\frac{2}{5}X-\frac{4}{5})$
5	1259	1	$(X^2-\frac{38}{3}X-\frac{22}{3})(X^2+\frac{44}{19}X+\frac{3}{19})(X^2+\frac{3}{11}X-\frac{19}{22})$
12	1259	2	$(X^2-26X-14)(X^2+\frac{28}{13}X+\frac{1}{13})(X^2+\frac{1}{7}X-\frac{13}{14})$
0	3	2	$(X^2-2X-2)(X^2+4X+1)(X^2+X-\frac{1}{2})$
0	54	1	$(X^2-4X-3)(X^2+3X+\frac{1}{2})(X^2+\frac{2}{3}X-\frac{2}{3})$
3	54	2	$(X^2-8X-5)(X^2+\frac{5}{2}X+\frac{1}{4})(X^2+\frac{2}{5}X-\frac{4}{5})$
1	66	2	$(X^2-5X-\frac{7}{2})(X^2+\frac{14}{5}X+\frac{2}{5})(X^2+\frac{4}{7}X-\frac{5}{7})$
2	2389	2	$(X^2-7X-\frac{9}{2})(X^2+\frac{18}{7}X+\frac{2}{7})(X^2+\frac{4}{9}X-\frac{7}{9})$

Although we already know $L_0^{(6)} = L_0^{(3)} \neq L_5^{(3)} = L_5^{(6)}$, we do not omit the degenerate cubic case $m, n \in \{0, 5\}$ on Table 2. By Theorem 3.4, the other sextic multi-resolvent polynomial $\mathcal{R}^j_{f_{m,n}}(X) = f_{A_j}^{C_6}(X)$, $(j \in \{1,2\}, j \neq i)$, is irreducible over $\mathbb{Q}$. By Theorem 4.3, we conclude that the overlap $L_m^{(6)} = L_n^{(6)}$ occurs only for the trivial cases $m = n$ and $m = -n-3$. □

5. Correspondence

The aim of this section is to establish the correspondence between isomorphism classes of the simplest sextic fields $L_m^{(6)}$ and non-trivial solutions to sextic Thue equations $F_m(x,y) = \lambda$ where λ is a divisor of $27(m^2+3m+9)$ as follows (cf. cubic case [H1] and quartic case [H2]):

Theorem 5.1. *Let $m \in \mathbb{Z}$ and $L_m^{(6)} = \mathrm{Spl}_{\mathbb{Q}} f_m^{C_6}(X)$. There exists an integer $n \in \mathbb{Z} \setminus \{m, -m-3\}$ such that $L_n^{(6)} = L_m^{(6)}$ if and only if there exists non-trivial solution $(x,y) \in \mathbb{Z}^2$, i.e. $xy(x+y)(x-y)(x+2y)(2x+y) \neq 0$, to $F_m(x,y) = \lambda$ where λ is a divisor of $27(m^2+3m+9)$.*

Proof. We apply Theorem 4.3 to the case $K = \mathbb{Q}$.

Assume that $L_m^{(6)} = L_n^{(6)}$ for $n \in \mathbb{Z} \setminus \{m, -m-3\}$. Then by Theorem 4.3 (iii) with $z = x/y$, there exist $x, y \in \mathbb{Z}$ with $\gcd(x,y) = 1$ such that

$$N = m + \frac{(m^2+3m+9)xy(x+y)(x-y)(x+2y)(2x+y)}{F_m(x,y)} \in \mathbb{Z} \tag{7}$$

where either $N = n$ or $N = -n-3$. The condition (7) occurs for only one of $N = n$ and $N = -n-3$ because only one of $f_{A_1}^{C_6}(X)$ and $f_{A_2}^{C_6}(X)$ in Theorem 4.3 (ii) has a linear factor over $\mathbb{Q}$. By (7), the assumption $n \in \mathbb{Z} \setminus \{m, -m-3\}$ implies $xy(x+y)(x-y)(x+2y)(2x+y) \neq 0$.

Now we should show that $F_m(x,y)$ divides $27(m^2+3m+9)$.

We use a standard method via resultant and the Sylvester matrix (cf. [PV00], [SWP08, Section 1.3], see also [Lan78, Theorem 6.1], [Lan83, Chapter 8, Section 5]). Put

$$h(z) := (m^2+3m+9)z(z+1)(z-1)(z+2)(2z+1)$$

and take $f_m^{C_6}(z) = F_m(z,1)$. We take the resultant

$$R_m := \mathrm{Res}_z(h(z), f_m^{C_6}(z)) = -3^9(m^2+3m+9)^6$$

of $h(z)$ and $f_m^{C_6}(z)$ with respect to z. The resultant R_m is also given by the determinant of the following modified Sylvester matrix of size 11×11:

$$S'(h, f_m^{C_6}) = \begin{bmatrix} a_5 & a_4 & \cdots & a_0 & 0 & h(z)z^5 \\ 0 & \ddots & \ddots & \cdots & \ddots & \vdots \\ 0 & 0 & a_5 & a_4 & \cdots & h(z) \\ b_6 & b_5 & \cdots & b_0 & 0 & f_m^{C_6}(z)z^4 \\ 0 & \ddots & \ddots & \cdots & \ddots & \vdots \\ 0 & 0 & b_6 & b_5 & \cdots & f_m^{C_6}(z) \end{bmatrix}$$

where $h(z) = \sum_{i=0}^{5} a_i z^i$, $f_m^{C_6}(z) = \sum_{i=0}^{6} b_i z^i$. By the cofactor expansion along the 11th column of the matrix $S'(h, f_m^{C_6})$, we have

$$h(z)(A_1 z^5 + \cdots + A_5 z + A_6) + f_m^{C_6}(z)(A_7 z^4 + \cdots + A_{10} z + A_{11}) = R_m. \tag{8}$$

Dividing the both sides of (8) by $-\mathrm{gcd}(A_1, \ldots, A_{11}) = -3^6(m^2 + 3m + 9)^5$, we have

$$h(z)p(z) + f_m^{C_6}(z)q(z) = 27(m^2 + 3m + 9)$$

where

$$\begin{aligned} p(z) &= 84z^5 - 42(4m + 1)z^4 - 112(3m + 11)z^3 \\ &\qquad + 7(22m - 153)z^2 + 2(161m + 219)z + 27m + 242, \\ q(z) &= (m^2 + 3m + 9)(-168z^4 - 336z^3 + 154z^2 + 322z + 27). \end{aligned}$$

Put $H(x, y) := y^6 h(x/y)$, $P(x, y) := y^5 p(x/y)$, $Q(x, y) := y^5 q(x/y)$. Then it follows from $z = x/y$ and $F_m(x, y) = y^6 f_m^{C_6}(x/y)$ that

$$H(x, y)P(x, y) + F_m(x, y)Q(x, y) = 27(m^2 + 3m + 9)y^{11}.$$

Hence by (7) we have

$$\frac{H(x, y)P(x, y)}{F_m(x, y)} + Q(x, y) = \frac{27(m^2 + 3m + 9)y^{11}}{F_m(x, y)} \in \mathbb{Z}.$$

Because the sextic forms $F_m(X, Y)$ and $H(X, Y)$ are invariants under the action of $\sigma : X \mapsto X + Y, Y \mapsto -X$, we may also get

$$\frac{H(x, y)P(x + y, -x)}{F_m(x, y)} + Q(x + y, -x) = \frac{27(m^2 + 3m + 9)(-x)^{11}}{F_m(x, y)} \in \mathbb{Z}.$$

We conclude that $F_m(x, y)$ divides $27(m^2 + 3m + 9)$ because $\mathrm{gcd}(x, y) = 1$.

Conversely if there exists $(x, y) \in \mathbb{Z}^2$ with $xy(x + y)(x - y)(x + 2y)(2x + y) \neq 0$ such that $F_m(x, y)$ divides $27(m^2 + 3m + 9)$ then we can take

$$N = m + \frac{(m^2 + 3m + 9)xy(x + y)(x - y)(x + 2y)(2x + y)}{F_m(x, y)} \in \mathbb{Q} \setminus \{m\}$$

which satisfies $L_N^{(6)} = L_m^{(6)}$ by Theorem 4.3. It follows from $\mathrm{Gal}_{\mathbb{Q}} f_m^{C_6}(X) \cong C_6$ or C_3 that $N \neq -m - 3$ (see also Table 1). Hence we have $N \in \mathbb{Q} \setminus \{m, -m - 3\}$.

We see that $N \in \mathbb{Z}$ as follows: If $x \equiv y \pmod 3$ then $xy(x + y)(x - y)(x + 2y)(2x + y) \equiv 0 \pmod{27}$. Hence we have $N \in \mathbb{Z} \setminus \{m, -m - 3\}$.

By a direct calculation, we obtain that if $x \not\equiv y \pmod 3$ then $F_m(x, y) \equiv 1 \pmod 3$. Hence $F_m(x, y)$ divides $m^2 + 3m + 9$ and $N \in \mathbb{Z} \setminus \{m, -m - 3\}$. □

References

[Ade01] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, 1761, Springer-Verlag, Berlin, 2001.

[AHK98] H. Ahmad, M. Hajja, M. Kang, *Negligibility of projective linear automorphisms*, J. Algebra **199** (1998), 344–366.

[Cha96] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), 283–291.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, 193, Springer-Verlag, New York, 2000.

[Enn91] V. Ennola, *Cubic number fields with exceptional units*, Computational number theory (Debrecen, 1989), 103–128, de Gruyter, Berlin, 1991.

[Gaa02] I. Gaál, *Diophantine equations and power integral bases. New computational methods*, Birkhäuser Boston, Inc., Boston, MA, 2002.

[GAP] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.10; 2007 (http://www.gap-system.org).

[Gir83] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), 289–307.

[Gra86] M. N. Gras, *Familles d'unités dans les extensions cycliques réelles de degré* 6 *de Q*, (French) Théorie des nombres, Années 1984/85–1985/86, Fasc. 2, Exp. No. 2, 27 pp., Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1986.

[Gra87] M. N. Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1987), 179–182.

[HH05] K. Hashimoto, A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74** (2005), 1519–1530.

[HM99] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), 165–181, Dev. Math., 2, Kluwer Acad. Publ., Dordrecht, 1999.

[H1] A. Hoshi, *On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields*, preprint, arXiv:0810.3374v3.

[H2] A. Hoshi, *On the simplest quartic fields and related Thue equations*, preprint, arXiv:1004.1960v2.

[HM07] A. Hoshi, K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation*, Proc. Japan Acad. Ser. A **83** (2007), 21–26.

[HM09a] A. Hoshi, K. Miyake, *A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation*, Number theory and applications, 65–104, Hindustan Book Agency, New Delhi, 2009.

[HM09b] A. Hoshi, K. Miyake, *On the field intersection problem of quartic generic polynomials via formal Tschirnhausen transformation*, Comment. Math. Univ. St. Pauli **58** (2009), 51–86.

[HM09c] A. Hoshi, K. Miyake, *On the field intersection problem of generic polynomials: a survey*, RIMS Kôkyûroku Bessatsu **B12** (2009), 231–247.

[HM10a] A. Hoshi, K. Miyake, *Some Diophantine problems arising from the isomorphism problem of generic polynomials*, Number Theory: Dreaming in Dreams, 87–105, Proceedings of the 5th China-Japan Seminar, World Sci. Publ., Singapore, 2010.

[HM10b] A. Hoshi, K. Miyake, *A note on the field isomorphism problem of $X^3 + sX + s$ and related cubic Thue equations*, Interdiscip. Inform. Sci. 16 (2010), 45–54.

[HM10c] A. Hoshi, K. Miyake, *On the field intersection problem of solvable quintic generic polynomials*, Int. J. Number Theory **6** (2010), 1047–1081.

[Kid05] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), 427–447.

[Kom04] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), 265–279.

[Lan78] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften, 231, Springer-Verlag, Berlin-New York, 1978.

[Lan83] S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.

[LPV98] G. Lettl, A. Pethö, P. Voutier, *On the arithmetic of simplest sextic fields and related Thue equations*, Number theory (Eger, 1996), 331–348, de Gruyter, Berlin, 1998.

[LPV99] G. Lettl, A. Pethö, P. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. **351** (1999), 1871–1894.

[Lou07] S. R. Louboutin, *Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields*, Math. Comp. **76** (2007), 455–473.

[Miy99] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Algebraic number theory (Hapcheon/Saga, 1996), Adv. Stud. Contemp. Math. (Pusan) **1** (1999), 137–142.

[Mor94] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), 183–208.

[Oga03] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, (Japanese) Algebraic number theory and related topics (Kyoto, 2002), Sūrikaisekikenkyūsho Kōkyūroku No. 1324, 217–224, 2003.

[Oka02] R. Okazaki, *Geometry of a cubic Thue equation*, Publ. Math. Debrecen **61** (2002), 267–314.

[Oka] R. Okazaki, *The simplest cubic fields are non-isomorphic to each other*, presentation sheet, available from `http://www1.doshisha.ac.jp/~rokazaki/papers.html`.

[PV00] D. Poulakis, E. Voskos, *On the practical solution of genus zero Diophantine equations*, J. Symbolic Comput. **30** (2000), 573–582.

[RV99] N. Rennert and A. Valibouze, *Calcul de résolvantes avec les modules de Cauchy*, Experiment. Math. **8** (1999), 351–366.

[Ren04] N. Rennert, *A parallel multi-modular algorithm for computing Lagrange resolvens*, J. Symbolic Comput. **37** (2004), 547–556.

[Rik02] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), 2215–2218.

[SWP08] J. R. Sendra, F. Winkler, S. Pérez-Díaz, *Rational algebraic curves. A computer algebra approach*, Algorithms and Computation in Mathematics, 22. Springer, Berlin, 2008.

[Sha74] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[Tog02] A. Togbé, *On the solutions of a family of sextic Thue equations*, Number theory for the millennium, III (Urbana, IL, 2000), 285–299, A K Peters, Natick, MA, 2002.

[Wak07a] I. Wakabayashi, *Number of solutions for cubic Thue equations with automorphisms*, Ramanujan J. **14** (2007), 131–154.

[Wak07b] I. Wakabayashi, *Simple families of Thue inequalities*, Ann. Sci. Math. Québec **31** (2007), 211–232.

Akinari Hoshi
Department of Mathematics
Rikkyo University
3–34–1 Nishi-Ikebukuro Toshima-ku
Tokyo, 171–8501, Japan
E-mail: `hoshi@rikkyo.ac.jp`
Web: `http://www2.rikkyo.ac.jp/web/hoshi/`